UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/927,928	08/09/2001	Rodric C. Fan	M-11702 US	6041

7590 05/22/2006

MacPherson Kwok Chen & Heid LLP
1762 Technology Dr.
Suite 226
San Jose, CA 95110

EXAMINER	
TESLOVICH, TAMARA	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/927,928	FAN ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/2806*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-11,15-17,20,25-27 and 29-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6, 8-11, 15-17, 20, 25-27, and 29-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on February 28, 2006 has been entered.

Claims 5, 7, 12-14, 18-19, 21-24, and 28 remain canceled.

Claims 1, 3, 6, 10, 29 and 31 have been amended

Claims 1-4, 6, 8-11, 15-17, 20, 25-27, and 29-35 are pending.

Response to Arguments

Applicant's arguments filed February 28, 2006have been fully considered but they are not persuasive.

In response to the Applicant's arguments on page 9 concerning Droge's alleged failure to disclose wherein the second encryption algorithm is applied in a manner such that the data packet is decrypted at the other end other wireless link and prior to the gateway forwarding to the wide area network, the Examiner respectfully disagrees and

calls the Applicant's attention to paragraphs 12-13, 36-37, and 42 wherein it is clearly stated:

"A method for securely transmitting and receiving data according to an embodiment of the present invention may comprise obtaining data on a first computer system for transmission. The data may be encrypted a first time such that the data is once encrypted ["encrypting a payload according to a first encryption algorithm"]. Subsequently, the first computer system may transmit the once encrypted data to a first interface device. The first interface device may receive the once encrypted data, packetize it ["adding a header to the encrypted payload to form a data packet"], and encrypt the packetized, once encrypted data a second time such that the data is twice encrypted ["encrypting the encrypted payload and the header of the data packet according to a second encryption algorithm, the second algorithm being an encryption algorithm used for secure communication over the wireless link"]. The first interface device may then transmit the packetized, twice encrypted data to a second interface device. The second interface device may receive the packetized, twice encrypted data and decrypt it and reconstruct it, or depacketize, the data such that the data is then once decrypted and reconstructed ["such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link"]. The second interface may then transmit the reconstructed, once decrypted data to a second computer system ["and prior to the gateway forwarding to the wide area network"]."

It is clear from paragraphs 36-37 and 42 of Droge that the transmission between the first and second interface devices could very well comprise a wired or wireless

network (par 36), and that the second interface device may comprise a transmission mechanism for the transmission of the data, now only once encrypted, over a transmission medium (par 37), which might be a PSTN or other type of dedicated communications link such as an ISDN, DSL, T1, dedicated wireless connection or the like (par 42).

Therefore, based on the above arguments, the Examiner respectfully maintains the rejections as set forth below and amended to reflect the Applicant's amendments.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-4, 6, 8-11, 15-17, 20, 25-27, and 29-35 are rejected under 35 U.S.C. 102(e) as being anticipated by Droge (U.S. Patent Application 09/841,168) and Schneier (Applied Cryptography, 2nd ed.). Schneier has been relied upon as a reference for features inherent to the Data Encryption Standard (DES).

As per claim 1, Droge discloses a method for transmitting data over a wireless link to a gateway providing access to a wide area network, the method comprising: encrypting a payload according to a first encryption algorithm; adding a header to the encrypted payload to form a data packet; encrypting the encrypted payload and the header of the data packet according to a second encryption algorithm, the second encryption algorithm being an encryption algorithm used for secure communication over

the wireless link, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding to the wide area network; and transmitting the encrypted data packet over the wireless link (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6).

As per claim 2, Droge discloses the method of claim 1, wherein the first algorithm uses a symmetric key (see Droge paragraph 53 reference "DES").

As per claim 3, Droge discloses the method of claim 1, further comprising: receiving the data packet at the gateway; decrypting data packet at the gateway according to the second algorithm; forwarding the recovered data packet to a computer on the wide area network; and decrypting the payload at the computer on the wide area network according to the first algorithm (see Droge paragraphs 36-40 and 51).

As per claim 4, Droge discloses the method of claim 1, wherein the first algorithm uses a symmetric session key (see Droge paragraph 53 reference "DES").

As per claim 6, Droge discloses a device for transmitting data over a wireless link to a gateway providing access to a wide area network, comprising: a wireless transceiver (see Droge paragraph 36 and 40); and an encryption engine coupled to the wireless transceiver for encrypting a payload according to a first encryption algorithm, adding a header to the payload to form a data packet, and encrypting the data packet according to a second algorithm, the second encryption algorithm being an algorithm for secured communications over a wireless link, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and

prior to the gateway forwarding to the wide area network (see Droge paragraphs 12-13, 36-37, 39-42, and 50 and figures 5,6).

As per claim 8, Droge discloses the device of claim 6, wherein the payload comprises location information regarding the location of the wireless device (see Droge paragraph 58, reference "IP header").

As per claim 9, Droge discloses the device of claim 6, wherein the first encryption algorithm employs a symmetric key (see Droge paragraph 53 reference "DES").

As per claim 10, Droge discloses a method for secure communication between a mobile device (see Droge paragraphs 61-62) and a server (see Droge paragraph 60) on a wide area network, comprising: generating a symmetric session key at the mobile device; encrypting the symmetric session key at the mobile device using a public key associated with the server; transmitting the encrypted session key to the server over a wireless link with a gateway to the wide area network; decrypting the encrypted session key at the server using a private key corresponding to the public key; encrypting a payload using the symmetric session key at the mobile device (see Droge paragraph 50 reference "algorithms that might be used to encrypt data at [the link layer] includes, without limitation, the DATA ENCRYPTION STANDARD (DES)"); adding a header to the payload to form a data packet at the mobile device; encrypting the encrypted payload and the header of the data packet using an encryption algorithm for secured communication over the wireless link to form an encrypted data packet at the mobile device, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding to the

wide area network; and transmitting the encrypted data packet from the mobile device to the gateway (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6, steps 92-102).

As per claim 11, Droge discloses the method of claim 10, further comprising: receiving the encrypted data at the gateway; decrypting the encrypted data packet at the gateway to recover a decrypted data packet, the decrypted data packet having the encrypted payload encrypted with the symmetric session key; forwarding the decrypted data packet to the server over the wide area network (see Droge figure 6, steps 104-114); decrypting the payload at the server using the decrypted session key (see Droge paragraph 50).

As per claim 15, Droge discloses the method of claim 10, wherein the payload includes location information (see Droge paragraph 58, reference "IP header").

As per claim 16, Droge discloses the method of claim 10, wherein the generating symmetric session key at the mobile device further comprises generating the symmetric key based on a random number (see Droge paragraph 53).

As per claim 17, Droge discloses the method of claim 10, wherein the encrypting a payload using the symmetric session key employs at least one of the encryption algorithms DESX or DES (see Droge paragraph 53).

As per claim 20, Droge discloses the method of claim 1, wherein the first algorithm comprises at least one of the encryption algorithms DES or DESX (see Droge paragraph 53).

As per claim 25, Droge discloses the method of claim 1, wherein the data packet includes location information (see Droge paragraph 58, reference "IP header").

As per claim 26, Droge discloses the method of claim 4, wherein the symmetric session key is generated based on a random number (see Droge paragraph 53).

As per claim 27, Droge discloses the device of claim 6 further comprising: a memory coupled to the encryption engine, the memory having a public key associated with a server on the wide area network stored therein (see Droge paragraph 39).

As per claim 29, Droge discloses a computer readable medium comprising program instructions for performing a method comprising: encrypting a payload according to a first encryption algorithm; adding a header to the encrypted payload to form a data packet; encrypting the encrypted payload and the header of the data packet according to a second encryption algorithm, the second encryption algorithm being an encryption algorithm used for secure communications over a wireless link, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding to the wide area network; transmitting the data packet to a server on a wide area network over a wireless link with a gateway providing access to the wide area network (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6).

As per claim 30, Droge discloses the computer readable medium of claim 29, wherein the first algorithm uses a symmetric key (see Droge paragraph 53 reference "DES").

As per claim 31, Droge discloses the computer readable medium of claim 29, the method further comprising: receiving the data packet at the gateway; decrypting the data packet at the gateway according to the second algorithm; forwarding the recovered data packet to a computer on the wide area network; and decrypting the payload at the computer on the wide area network according to the first algorithm (see Droge paragraphs 36-40 and 51).

As per claim 32, Droge discloses the computer readable medium of claim 29, wherein the first algorithm uses a symmetric session key (see Droge paragraph 53 reference "DES").

As per claim 33, Droge discloses the computer readable medium of claim 29, wherein the first algorithm comprises at least one of the encryption algorithms DESX or DES (see Droge paragraph 53).

As per claim 34, Droge discloses the computer readable medium of claim 29 wherein the data packet includes location information (see Droge paragraph 58, reference "IP header").

As per claim 35, Droge discloses the computer readable medium of claim 32 wherein the symmetric session key is generated based on a random number (see Droge paragraph 53).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

May 14, 2006
TT/ELM

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER